

Deep Security Agent ユーザーズガイド 第7版

2024年 8月 日本電気株式会社

目次

概要

1.ログイン

- ・ログイン手順

2.ダッシュボード

- ・概要
- ・表示期間の変更
- ・ウィジェット(表示項目)の追加・削除
- ・タブの追加

3.アラート

- ・概要
- ・アラートの設定

4.イベントとレポート

- ・概要
- ・レポートの生成

5.コンピュータ

- ・概要
- ・Agentの無効化
- ・Agentの有効化
- ・グループの設定
- ・推奨スキュンの実施

6.ポリシー

- ・概要
- ・ポリシーの継承
- ・侵入防御ルール手動適用の注意点
- ・侵入防御ルールを手動適用する手順

7.管理

- ・概要
- ・ユーザの管理
- ・ユーザの新規作成
- ・アップデート

8.Appendix

- ・コマンドラインの利用
- ・利用するカーネルに対応したKSPがインポートされているかを確認する方法

9.注意事項

10.問い合わせ先

概要

- ◆ 本資料はサーバセキュリティサービス利用者向けガイドになります。
- ◆ 詳細につきましては、サポート情報にてご確認をお願いします。

1.ログイン

◆ ログイン手順

- サーバセキュリティサービスのDeep Securityは、Webブラウザで管理コンソールにアクセスして管理します。

■ ログイン手順は以下となります。

[1] <https://serversecurity-nec.jp/SignIn.screen>にアクセスして下さい。

[2] 「アカウント名」「ユーザ名」「パスワード」を入力してログイン。

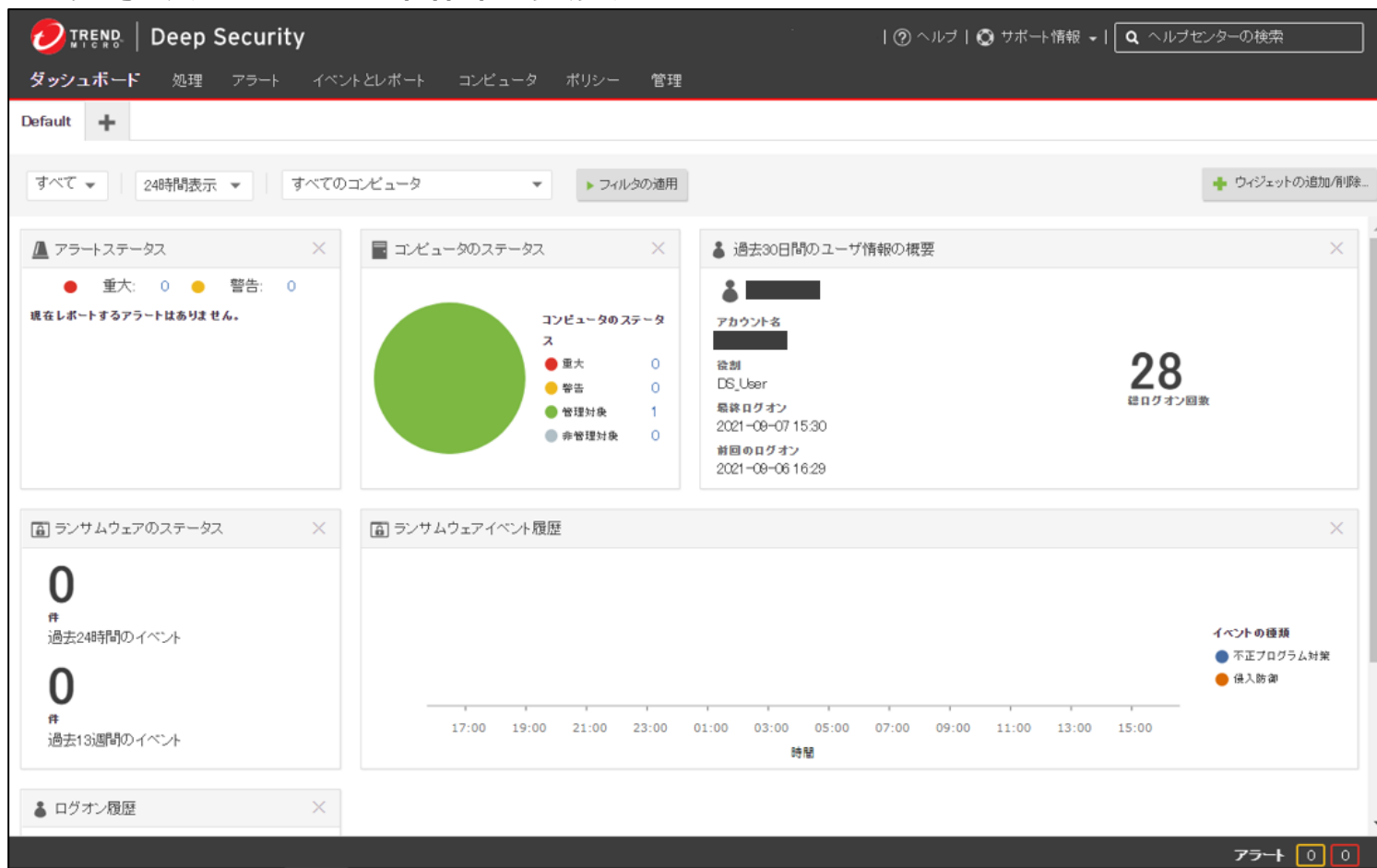
※初期設定はライセンス証書に記載されています。



2. ダッシュボード

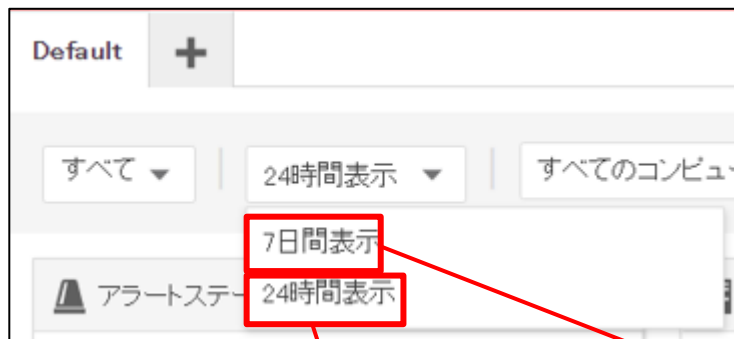
◆ 概要

- [ダッシュボード]には、システムの状態を一目で理解できるビューがあります。これらの表示項目などは、自由に変更できます。



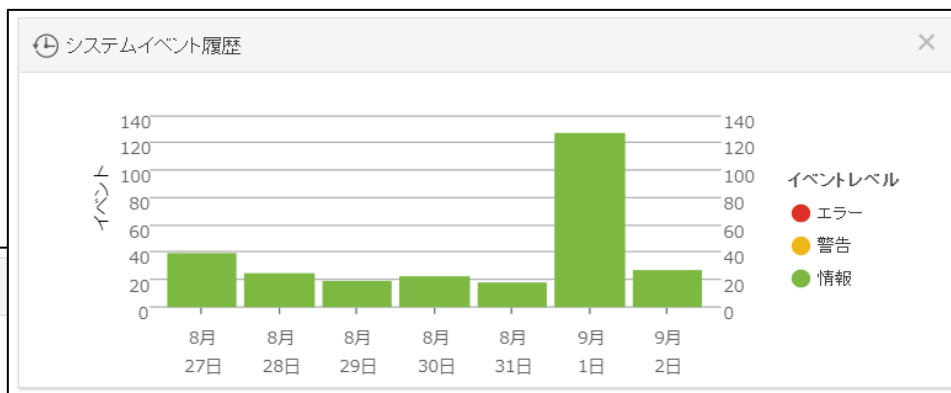
2. ダッシュボード

◆ 表示期間の変更

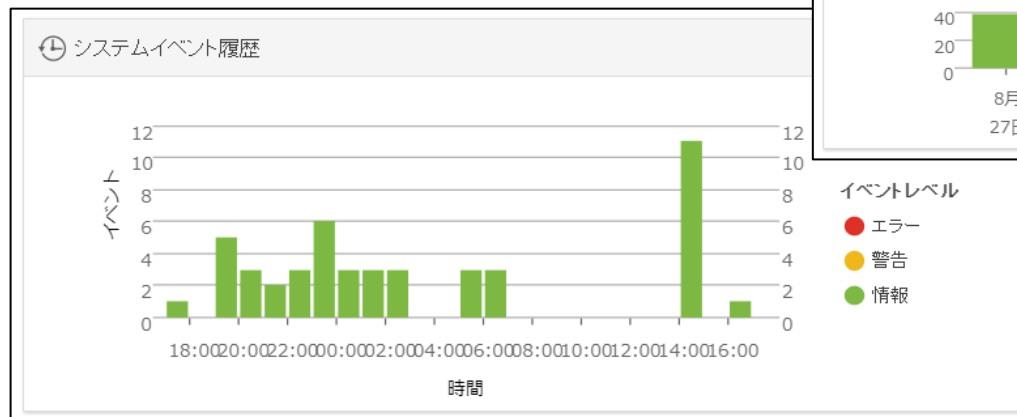


ウィジェットの日時表示範囲
を24時間表示 or 7日間表示
に切り替えることができます。

7日間表示



24時間表示



2.ダッシュボード

◆ ウィジェット(表示項目)の追加・削除

ウィジェットの追加・削除をクリックすると、表示するウィジェットを選択することができます。

また、ドラッグすることでウィジェットを任意の配置に変更できます。

ダッシュボードのウィジェット一覧:

- アラートステータス
- コンピュータのステータス
- システムイベント履歴
- ランサムウェアのステータス
- IPSのアクティビティ (防御)
- ソフトウェアアップデート
- 不正プログラム対策のステータス (コンピュータ)

2.ダッシュボード

◆ タブの追加

The image shows the Trend Micro Deep Security interface. The top navigation bar includes 'ダッシュボード' (Dashboard), '処理' (Processing), 'アラート' (Alerts), and 'イベントとレポート' (Events and Reports). The main dashboard area has a 'Default' tab with a '+' icon next to it. A red box highlights this '+' icon, and a red arrow points from it to a modal window titled '新規ダッシュボードの追加' (Add New Dashboard). The modal window contains the text '新規ダッシュボード名:' (New Dashboard Name:) followed by a text input field containing '不正プログラム対策' (Malware Protection). Below this is a checkbox labeled '現在のダッシュボードの複製' (Duplicate current dashboard). At the bottom of the modal are '追加' (Add) and 'キャンセル' (Cancel) buttons. A second red arrow points from the '+' icon in the main dashboard to the same '+' icon in a second screenshot below. This second screenshot shows the dashboard with the '不正プログラム対策' tab added. A blue box at the bottom left contains the text: '[+]をクリックし、タブを追加する事で、機能毎に表示項目を分けるなどカスタマイズ可能です。' (By clicking the [+] button, you can add tabs, allowing for customization such as separating display items by function.)

Default +

すべて 24時間表示 すべてのコンピュータ

アラートステータス

新規ダッシュボードの追加

新規ダッシュボード名: 不正プログラム対策

☐ 現在のダッシュボードの複製

追加 キャンセル

ヘルプ サポート情報 ヘルプセンターの検索

ダッシュボード 処理 アラート イベントとレポート コンピュータ ポリシー 管理

Default × 不正プログラム対策 × +

すべて 24時間表示 すべてのコンピュータ フィルタの適用 ウィジェットの追加/削除

不正プログラム対策の保護ステータス

不正プログラム対策のステータス (不正プログラム)

検出された不正プログラムのトップ5

取得可能な情報はありません

不正プログラム対策のステータス (コンピュータ)

検出された不正プログラムのトップ5

[+]をクリックし、タブを追加する事で、機能毎に表示項目を分けるなどカスタマイズ可能です。

3.アラート

◆ 概要

- [アラート]画面には、有効なアラートがすべて表示されます。
[アラートの設定]を行うことで、表示有無や重要度を任意に変更できます。

The screenshot shows the Trend Micro Deep Security web interface. The top navigation bar includes 'ダッシュボード', '処理', 'アラート', 'イベントとレポート', 'コンピュータ', 'ポリシー', and '管理'. The 'アラート' (Alerts) section is active. Below the navigation bar, there are filters for 'アラート' (Alerts) and 'コンピュータ' (Computers). A table displays a single alert: '警告' (Warning) at '2021-09-02 17:22' regarding 'Agent/Applianceのアップグレード推奨 (新しいバージョンが使用可能)' (Agent/Appliance upgrade recommendation (new version available)). The bottom right corner shows a summary: 'アラート 1 0'.

時刻	重要度	アラート	対象	対象箇所
2021-09-02 17:22	警告	Agent/Applianceのアップグレード推奨 (新しいバージョンが使用可能)		

3.アラート

◆ アラートの設定



アラート設定 グループ化しない		
プロパティ...		
アラート	重要度	オン
ファイアウォールエンジンがオフライン	重大	✓
ファイアウォールルールの推奨	警告	✓
ファイアウォールルールアラート	警告	✓
ファイルで不正プログラムを検索できませんでした	警告	✓
ポリシー送信の失敗	重大	✓
メンテナンスモード - オン	警告	✓
ユーザのロックアウト	警告	✓
ユーザパスワードがまもなく有効期限切れ	警告	✓
ルールのアップデートが利用可能	警告	✓
不正プログラムの予約検索がスキップされました	警告	✓
不正プログラム対策アラート	警告	✓
不正プログラム対策エンジンがオフライン	重大	✓
不正プログラム対策コンポーネントのアップデートの失敗	警告	✓
不正プログラム対策コンポーネントの障害	重大	✓
不正プログラム対策モジュールで検出ファイル保存用の最大ディスク容量...	警告	✓
不正プログラム対策保護がいつか、期限切れ	警告	✓
不正プログラム対策保護でコンピュータの再起動が必要	重大	✓

アラート情報

アラート: 不正プログラム対策アラート

説明: 1台以上のコンピュータで、アラートを発するように設定された不正プログラム検索設定によってイベントが発生しました。

消去可能: はい

☒ オン
オンのとき、条件を満たす場合、アラートが発令されます。

オプション

重要度: 警告

☐ 重大 [このルールでアラート]

☒ 警告 このアラートの発令時、通知のメールを送信する

☒ このアラートの条件が変更になった場合 (アイテムの数など)、通知のメールを送信する

☒ このアラートが存在しなくなったとき、通知のメールを送信する

☐ オフ
オフのとき、アラートは発令されません。この条件でアラートが発令されないようにするには、この設定を使用します。

OK キャンセル 適用

4. イベントとレポート

◆ 概要

- [イベントとレポート]では、各種イベントの表示、レポートの作成を行えます。

The screenshot displays the 'Deep Security' interface, specifically the 'イベントとレポート' (Event and Report) section. The top navigation bar includes 'ダッシュボード', '処理', 'アラート', 'イベントとレポート', 'コンピュータ', 'ポリシー', and '管理'. The 'イベントとレポート' section is active, showing a list of system events. The interface includes filters for 'システムイベント' (System Event) and 'グループ化しない' (Do not group), a search bar, and a refresh button. The event list table is as follows:

時刻	レベル	イベントID	イベント	タグ	イベント送信...	対象	処理実行者
2021-08-03 14:08:12	情報	600	ユーザのログオン		Manager		
2021-08-02 17:03:48	情報	601	ユーザのログオフ		Manager		システム
2021-08-02 17:03:33	情報	600	ユーザのログオン		Manager		
2021-08-02 16:46:52	情報	2204	セキュリティアップデート: Agent/Appliance...		Agent		システム
2021-08-02 16:46:52	情報	276	アップデート: 概要情報		Manager		システム
2021-08-02 16:40:19	情報	273	セキュリティアップデート: セキュリティアッ...		Manager		システム
2021-08-02 16:40:19	情報	1600	Relayグループのアップデートの要求		Manager	初期設定のRelayグル...	システム
2021-08-02 16:40:19	情報	564	予約タスクの開始		Manager	コンポーネントアップデ...	システム
2021-08-02 14:47:32	情報	601	ユーザのログオフ		Manager		システム
2021-08-02 14:18:46	情報	600	ユーザのログオン		Manager	USER01	USER01

4. イベントとレポート

◆ レポートの作成

レポートの生成から、不正プログラム検出件数等のレポートを出力できます。

不正プログラム対策	検出モード	防衛モード	合計	割合
	検出モード	防衛モード	検出モード+防衛モード	防衛モード/合計
不正プログラム対策	検出: 0 検出不能: 0	検出: 0 検出不能: 0	0	0 / 0 (なし)
ファイアウォール	ルール: 0 設定: 0 合計: 0	ルール: 0 設定: 0 合計: 0	0	0 / 0 (なし)
攻撃の予兆検索	OSのフィンガープリント ネットワークまたはポート検査 TOP Nファイル検査 TOP Nプロセス検査 合計: 0	なし	0	なし
攻撃コード	重大: 0 高: 0 中: 0 低: 0 合計: 0	重大: 0 高: 0 中: 0 低: 0 合計: 0	0	0 / 0 (なし)
脆弱性	重大: 0 高: 0 中: 0 低: 0 合計: 0	重大: 0 高: 0 中: 0 低: 0 合計: 0	0	0 / 0 (なし)
スマート	重大: 0 高: 0 中: 0 低: 0 合計: 0	重大: 0 高: 0 中: 0 低: 0 合計: 0	0	0 / 0 (なし)
ポリシー	重大: 0 高: 0 中: 0 低: 0 合計: 0	重大: 0 高: 0 中: 0 低: 0 合計: 0	0	0 / 0 (なし)
ルールベース以外	検出: 0 検出不能: 0 合計: 0	検出: 0 検出不能: 0 合計: 0	0	0 / 0 (なし)

5.コンピュータ

◆ 概要

- [コンピュータ]では、推奨スキャンの実施や表示名変更など各コンピュータの管理を行います。



5.コンピュータ

◆ Agentの無効化

- 処理＞無効化より、Agentを無効化できます。

コンピュータ

サブグループを含む ▼ グループ別 ▼

追加 ▼ 削除... 詳細... 処理 ▼ イベント ▼ エクスポート ▼ 列...

名前 ▲ 説明 プラットフォーム ポリシー ステータス

▼ コンピュータ (1)

Microsoft Wind... サーバセキュ... 管理対象 (オンライン)

すべて選択 (1)

選択したアイテムをCSV形式でエクスポート
選択したアイテムをXML形式でエクスポート

処理
イベント
削除...
詳細...

無効化

ポリシーの送信
セキュリティアップデートのダウンロード
セキュリティアップデートのロールバック
警告/エラーのクリア
Agent/ソフトウェアのアップグレード...

非管理対象(有効化が必要)

Trend Micro Deep Security

Agentのステータス

Agent	有効化が必要
不正プログラム対策	保護できません
Webレピュテーション	保護できません
ファイアウォール	保護できません
侵入防御	保護できません
変更監視	保護できません
セキュリティログ監視	保護できません
アプリケーションコントロール	保護できません

コンポーネント

Agentが無効化されると「Deep Security Notifier」のコンソールにて、Agentのステータスが「有効化が必要」になります。(Windowsのみ)

不正プログラムの検出時に通知(M)
不正なWebサイトの検出時に通知(W)
コンソールを開く(O)
終了(X)

通知
[x] 不正プログラムの検出時に通知(M)
[x] 不正なWebページのブロック時に通知(W)

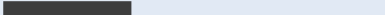
詳細
イベントの表示(V)...

OK キャンセル 適用(A)

5.コンピュータ

◆ Agentの有効化

- 無効化したAgentを有効化する場合、対象のサーバ上で有効化コマンドを実行する必要があります。

名前 ^	説明	プラットフォ...	ポリシー	ステータス
▼ コンピュータ (1)				
		不明	サーバセキュ...	● 非管理対象 (有効化が必要)

[1]有効化コマンドの作成

※手順は導入手順書を確認

[2]有効化するサーバ上で有効化コマンドを実行する。

インストールスクリプト

☒ インストール後にAgentを自動的に有効化 (セキュリティポリシーを適用する場合は必ず有効化してください)

セキュリティポリシー:

コンピュータグループ:

Relayグループ:

Deep Security Managerへの接続に使用するプロキシ:

Relayへの接続に使用するプロキシ:

☐ Deep Security ManagerのTLS証明書を確認 [詳細を表示](#)

☐ Agentのインストールのデジタル署名を確認 [詳細を表示](#)

☐ Trend Micro Vision One (XDR) 用のTrend Micro Endpoint Baselineをインストール [詳細を表示](#)

☒ 有効化コマンドの作成

&\$Env:ProgramFiles\Trend Micro\Deep Security Agent\dsa_control -r
&\$Env:ProgramFiles\Trend Micro\Deep Security Agent\dsa_control -a \$ACTIVATIONURL -t "tenantID" -p "policyid:1" -u "token"

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Program Files\Trend Micro\Deep Security Agent
C:\Program Files\Trend Micro\Deep Security Agent>dsa_control -a dsm://... -t "tenantID:1" -p "policyid:1" -u "token"

Activation will be re-attempted 30 time(s) in case of failure
dsa_control
HTTP Status: 200 - OK
Response
Attempting to connect to https://...
SSL handshake completed successfully - initiating command session.
Connected with EDDHE-RSA-AES256-GCM-SHA384 to peer at ...
Received a 'GetHostInfo' command from the manager.
Received a 'SetDSMCert' command from the manager.
Received a 'SetAgentCredentials' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'SetAgentStatus' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetHostMetadata' command from the manager.
Received a 'GetAgentStatus' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetComponentInfo' command from the manager.
Received a 'GetDockerVersion' command from the manager.
Received a 'SetURIInformation' command from the manager.
Received a 'SetSecurityConfiguration' command from the manager.
Received a 'GetAgentEvents' command from the manager.
Received a 'GetAgentStatus' command from the manager.
Received a 'UpdateComponent' command from the manager.
Received a 'SetDSMCert' command from the manager.
Command session completed.
```

※Windowsでの実行例

5.コンピュータ

◆ グループの設定

- 管理コンソール左側のコンピュータを右クリックすることで新規にグループを追加できます。
- グループを割り当ては、コンピュータの詳細(対象をダブルクリック)より行います。

The screenshot displays the Trend Micro Deep Security management console. The left sidebar shows the navigation menu with 'スマートフォルダ' (Smart Folders) and 'コンピュータ' (Computers) highlighted. The main area shows the 'コンピュータ' (Computers) section with a table listing existing computers. A red box highlights the 'コンピュータ' (Computers) option in the left sidebar. Another red box highlights the 'コンピュータ' (Computers) option in the 'グループ' (Groups) dropdown menu on the right side of the console. The right side of the console shows the details of a selected computer, including its name, IP address, and operating system (Microsoft Windows Server 2012 (64 bit) Build 9200). The 'グループ' (Groups) dropdown menu is open, showing a list of groups, with 'コンピュータ' (Computers) selected. The 'DBサーバ' (DB Server) and 'Webサーバ' (Web Server) groups are also visible. The bottom of the console shows the '保存' (Save) and '閉じる' (Close) buttons.

5.コンピュータ

◆ 推奨スキャンの実施

[1]「コンピュータ」タブより、対象サーバを右クリック。

[2]処理> 推奨設定の検索をクリック。

[3]ステータス列に「推奨設定の検索の保留中(ハートビート)」が表示され、数分後に推奨設定が実行されます。

[4]推奨スキャン実施後、対象コンピュータをダブルクリックし、侵入防御を選択。一般タブにて割り当てられている侵入防御ルールを確認できます。

The screenshot displays the NEC security management console interface. On the left, the 'コンピュータ' (Computer) tab is selected, showing a list of computers. A context menu is open for a selected computer, with the '処理' (Process) option highlighted. The '推奨設定の検索' (Search for recommended settings) option is also highlighted. Below the context menu, a 'タスク' (Task) section shows '推奨設定の検索の保留中(ハートビート)' (Recommended settings search on hold (heartbeat)).

On the right, the '侵入防御' (Intrusion Prevention) settings page is shown. The '一般' (General) tab is selected, displaying the status of the intrusion prevention system. Below this, a table lists the assigned intrusion prevention rules.

名前	アプリケーションの種類	優先度	重要度	モード	種類	カテゴリ	CVE
1000128 - HTTP Protocol Decoding	Web Server Common	1 - 低	重大	防御	スマート	Webアプリケーションの...	CVE-2004-1...
1004715 - HTTP Web Client Dec...	Web Client Common	1 - 低	重大	防御	スマート	脆弱性と攻撃コード	なし
1004790 - Identified Dighotar Ce...	Web Client SSL	2 - 標準	重大	防御	スマート	脆弱性と攻撃コード	なし
1005040 - Identified Revoked Ce...	Web Client SSL	2 - 標準	重大	防御	スマート	脆弱性と攻撃コード	なし

5.コンピュータ

- 推奨スキャン完了後、「未解決の推奨設定」がある場合は下記の手順でルール割り当てが可能です。※自動的に適用できないルールがございます。

[1]「割り当て/割り当て解除...」をクリック。

[2]侵入防御ルールの中央のボックスから「割り当てを推奨」を選択

[3]表示されたルール左側のチェックボックスをチェックして、OKボタンを押す。

The screenshot displays the NEC security management interface. On the left, a sidebar shows '現在割り当てられている侵入防御ルール' (Intrusion Prevention Rules Currently Assigned) and '推奨設定' (Recommended Settings). The '推奨設定' section indicates '未解決の推奨設定: 1個の追加ルールの割り当て' (Unresolved Recommended Settings: Assignment of 1 additional rule). The main area shows a list of rules, including '1000128 - HTTP Protocol Decoding' and '1004715 - HTTP Web Client Dec...'. A red box highlights the '割り当て/割り当て解除...' button. A red arrow points from this button to a dropdown menu in the center, which lists options: 'すべて', '割り当てあり', '割り当てなし', '割り当てを推奨' (highlighted), and '割り当て解除を推奨'. Another red arrow points from the '割り当てを推奨' option to a rule entry '1007596 - Identified Possible Ra...'. A red box highlights the checkbox for this rule. A red arrow points from the checkbox to the 'OK' button at the bottom right. A blue box contains a tip: '(Tips) 一部の侵入防御ルールは、誤検知のリスクがある等の理由で、自動で割り当てされません。適用後1週間「検知」モードで様子を見る等の運用もご検討ください。' (Some intrusion prevention rules are not automatically assigned due to risks of false detection, etc. Please consider operations such as monitoring in 'Detection' mode for 1 week after application, etc.).

現在割り当てられている侵入防御ルール

すべて

割り当て/割り当て解除...

名前

アプリケーションの種類

優先度

1000128 - HTTP Protocol Decoding Web Server Common 1 - 低

1004715 - HTTP Web Client Dec... Web Client Common 1 - 低

1004790 - Identified Diginotar Ce... Web Client SSL 2 - 標準

1005040 - Identified Revoked Ce... Web Client SSL 2 - 標準

1005307 - Identified Fraudulent ... Web Client SSL 2 - 標準

推奨設定

現在のステータス: 24個の侵入防御ルールが割り当て

前回の推奨設定の検索: 2021-09-03 17:12

未解決の推奨設定: 1個の追加ルールの割り当て

侵入防御の推奨設定を自動的に適用(可能な場合): 継承 (はい)

推奨設定の検索

推奨設定の検索のキャンセル

侵入防御ルール

すべて

割り当てを推奨

アプリケーションの種類別

新規

削除

プロパティ

名前

アプリケーションの種類

名前

カテゴリ

CVE

CVSSスコ...

すべて

割り当てあり

割り当てなし

割り当てを推奨

割り当て解除を推奨

1007596 - Identified Possible Ra... 2 - 標準 ● 重大 検出のみ スマート 不審なネットワークアク... なし

割り当てを推奨

アプリケーションの種類別

すべて

割り当てあり

割り当てなし

割り当てを推奨

割り当て解除を推奨

種類

スマート

OK

キャンセル

(Tips)

一部の侵入防御ルールは、誤検知のリスクがある等の理由で、自動で割り当てされません。適用後1週間「検知」モードで様子を見る等の運用もご検討ください。

6.ポリシー

◆ 概要

- ポリシーの確認・編集や、侵入防御ルールの確認等を行えます。

TREND MICRO | Deep Security

ヘルプ | サポート情報 | ヘルプセンターの検索

ダッシュボード 処理 アラート イベントとレポート コンピュータ **ポリシー** 管理

ポリシー

新規 削除... 詳細... 複製 エクスポート

サーバセキュリティサービス_ポリシー

ポリシーをダブルクリックする事で詳細を開けます。

※ポリシーを変更する際には、「サーバセキュリティサービス_ポリシー」を複製または継承元として新規にポリシーを作成し、対象のコンピュータに適用することを推奨します。

アラート 0 0

6.ポリシー

◆ ポリシーの継承

- 親ポリシーを元に作成された子ポリシーは、設定変更しない場合、ポリシー設定画面にて「(継承)」と表記されます

ポリシー: テストポリシー > テストポリシー02 ヘルプ

概要 | 不正プログラム対策 | 侵入防御 | インタフェースの種類 | 設定 | オーバーライド

一般 | Smart Protection | Connected Threat Defense | 詳細 | 検出ファイル | 不正プログラム対策イベント

不正プログラム対策

不正プログラム対策のステータス: 継承 (オン) リアルタイム

リアルタイム検索

☐ 継承

不正プログラム検索設定: Default Real-Time Scan Configuration 編集

スケジュール: Every Day All Day 編集

手動検索

☐ 継承

不正プログラム検索設定: Default Manual Scan Configuration 編集

予約検索

☐ 継承

不正プログラム検索設定: Default Scheduled Scan Configuration 編集

保存 閉じる

6.ポリシー

◆ 侵入防御ルール手動適用の注意点

■ 推奨設定の検索使用時に任意のルールを手動で割り当てする場合

推奨設定の検索にて、[侵入防御の推奨設定を自動的に適用（可能な場合）:]を「はい」に設定している場合、コンピュータの詳細画面から、コンピュータレベルで手動適用した侵入防御ルールが、自動的に割り当て解除される場合があります。

推奨設定の検索使用時に任意のルールを手動で割り当てする場合は、ポリシーの設定画面から、ポリシーレベルで任意のルールを割り当ててください。

参考情報

<https://success.trendmicro.com/ja-jp/solution/ka-0001819>

6.ポリシー

[侵入防御の推奨設定を自動的に適用 (可能な場合):]の設定は、「ポリシー」または「コンピュータ」の詳細ページで確認できます。

- ・「ポリシー」→対象のポリシーをダブルクリックして詳細画面を表示。
 - ・「コンピュータ」→対象のコンピュータをダブルクリックして詳細画面を表示。
- 左ペインの「侵入防御」を選択し、「一般」タブを参照する。(共通)

ポリシー: サーバセキュリティサービスポリシー ヘルプ

概要 一般 詳細 侵入防御イベント

不正プログラム対策

侵入防御

インタフェースの種類

設定

オーバーライド

コンテナの保護

コンテナのネットワークトラフィックの検索: 初期設定 (はい)

現在割り当てられている侵入防御ルール

すべて

割り当て/割り当て解除... プロパティ... エクスポート... アプリケーションの種類... 列...

名前	アプリケーションの種類	優先度	重要度	モード	種類	カテゴリ
(リストにアイテムがありません)						

推奨設定

現在のステータス: 0個の侵入防御ルールが割り当てられています

未解決の推奨設定: 59個の追加ルールの割り当て

侵入防御の推奨設定を自動的に適用 (可能な場合): はい

保存 閉じる

6.ポリシー

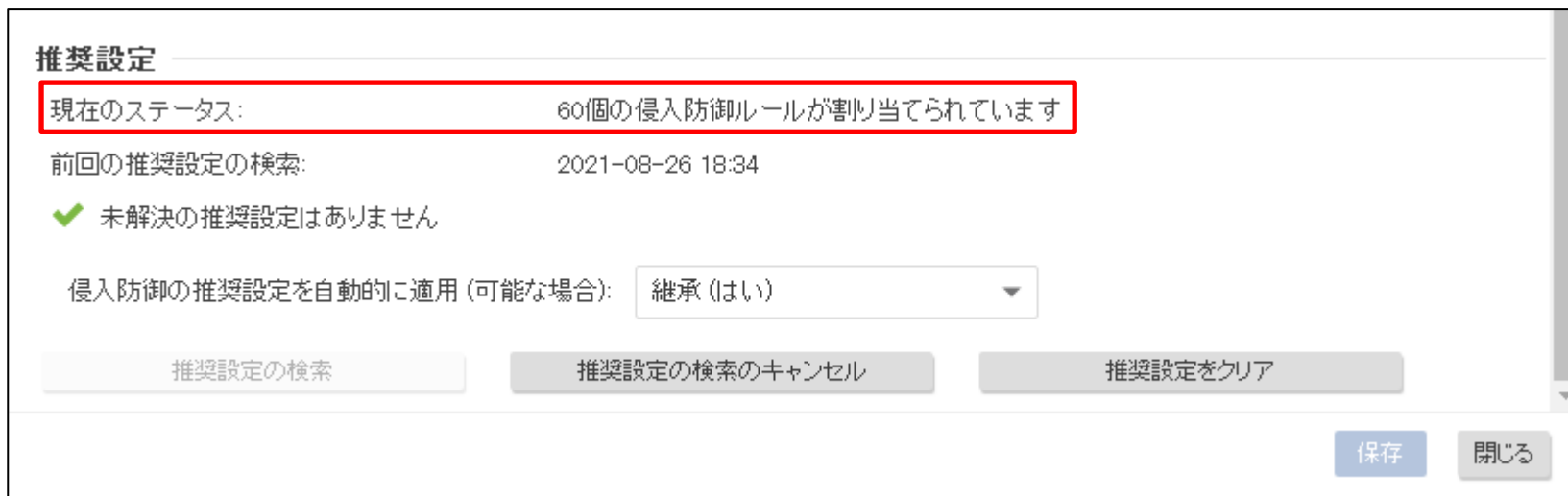
◆ 侵入防御ルールを手動適用する手順

1. 現在割り当てられているルールの確認

侵入防御ルールを手動適用した後、割り当てられていることを確認するために、以下の手順で対象のコンピュータの詳細画面を開き、現在割り当てられている侵入防御ルールの数と、割り当てるルールの適用状況、設定状況が分かるように、メモまたは画面キャプチャの取得をしてください。

- 現在割り当てられている侵入防御ルール数の確認

[コンピュータ] → 対象のコンピュータの[詳細] → [侵入防御] → [一般]タブを参照



推奨設定

現在のステータス: 60個の侵入防御ルールが割り当てられています

前回の推奨設定の検索: 2021-08-26 18:34

✓ 未解決の推奨設定はありません

侵入防御の推奨設定を自動的に適用 (可能な場合): 継承 (はい)

推奨設定の検索 推奨設定の検索のキャンセル 推奨設定をクリア

保存 閉じる

6.ポリシー

- 割り当てるルール適用状況の確認

対象のコンピュータの[詳細]から、以下の手順でルールの適用状況を確認。

名前	優先度	重要度	モード	種類	カテゴリ	CVE	CVSS
▼ ActiveMQ OpenWire (1)							
1010428 - Apache ActiveMQ U...	2 - 標準	中	防御	攻撃コード	なし	CVE-2015-...	5.4
▼ Advanced Message Queuing Protocol (AMQP) (1)							
1009126 - Pivotal Spring AMQ...	2 - 標準	高	防御	攻撃コード	脆弱性と攻撃コード	CVE-2017-...	7.5
▼ Alibaba Nacos (1)							
1010971 - Alibaba Nacos AuthF...	2 - 標準	高	防御	攻撃コード	脆弱性と攻撃コード	CVE-2021-...	7.5
▼ Apache JServ Protocol (2)							
1010184 - Identified Apache JS...	2 - 標準	高	検出のみ	スマート	脆弱性と攻撃コード	CVE-2020-...	7.5

6.ポリシー

- 割り当てるルールの設定状況の確認

ルールの変更される場合は、対象のルールの[プロパティ]を開き、現在の設定状況がわかるように、メモまたは画面キャプチャを取得してください。

The screenshot displays the 'Intrusion Defense Rule' management interface. On the left, a table lists several rules. The rule '1010428 - Apache ActiveMQ U...' is highlighted with a red box. A red arrow points from this rule to the 'Intrusion Defense Rule Property' window on the right.

名前	優先度	重要度	モード	種類	カテゴリ
ActiveMQ OpenWire (1)					
1010428 - Apache ActiveMQ U...	2 - 標準	中	防御	攻撃コード	なし
Advanced Message Queuing Protocol (AMQP) (1)					
1009126 - Pivotal Spring AMQ...	2 - 標準	高	防御	攻撃コード	脆弱性と
Alibaba Nacos (1)					
1010971 - Alibaba Nacos AuthF...	2 - 標準	高	防御	攻撃コード	脆弱性と
Apache JServ Protocol (2)					
1010184 - Identified Apache JS...	2 - 標準	高	検出のみ	スマート	脆弱性と

The 'Intrusion Defense Rule Property' window for 'Apache ActiveMQ Unsafe Deserialization' shows the following details:

- 名前:** Apache ActiveMQ Unsafe Deserialization
- 説明:** Apache ActiveMQ is prone to deserialization vulnerability, as it does not restrict the classes that can be serialized in the broker, which allows remote attackers to execute
- 最小 Agent/Appliance バージョン:** 4.0.0.0
- 詳細:**
 - アプリケーションの種類: ActiveMQ OpenWire
 - 優先度: 2 - 標準
 - 重要度: 中
 - モード: 継承 (防御)

Buttons at the bottom: OK, キャンセル, 適用

6.ポリシー

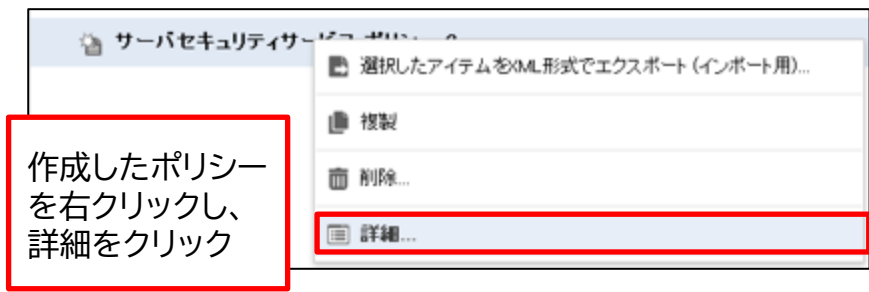
2. [サーバセキュリティサービス_ポリシー]を複製 [ポリシー]タブ→[ポリシー]



6.ポリシー

3. 複製したポリシーに侵入防御ルールを割り当てる

作成したポリシーを右クリックし、詳細をクリック



ポリシー: サーバセキュリティサービスポリシー_2

概要 不正プログラム対策 侵入防御 インタフェースの種類 設定 オーバーライド

一般 詳細 侵入防御イベント

侵入防御

侵入防御のステータス: オン

侵入防御の動作

☒ 防御 ☐ 検出

コンテナの保護

コンテナのネットワークトラフィックの検索:

現在割り当てられている侵入防御ル

すべて

割り当て/割り当て解除...

侵入防御ルール

新規 削除 プロパティ 複製 エクスポート アプリケーションの種類 列

名前	優先度	重要度	モード	種類	カテゴリ	CVE	CVSS
▼ ActiveMQ OpenWire (1)							
☒ 1010428 - Apache ActiveMQ U...	2 - 標準	中	防御	攻撃コード	なし	CVE-2015-...	5.4
▼ Advanced Message Queuing Protocol (AMQP) (1)							
☐ 1009126 - Pivotal Spring AMQ...	2 - 標準	高	防御	攻撃コード	脆弱性と攻撃コード	CVE-2017-...	7.5
▼ Alibaba Nacos (1)							
☐ 1010971 - Alibaba Nacos AuthF...	2 - 標準	高	防御	攻撃コード	脆弱性と攻撃コード	CVE-2021-...	7.5
▼ Apache JServ Protocol (2)							
☐ 1010184 - Identified Apache JS...	2 - 標準	高	検出のみ	スマート	脆弱性と攻撃コード	CVE-2020-...	7.5
☐ 1010361 - Apache Tomcat Loc...	2 - 標準	中	防御	脆弱性	脆弱性と攻撃コード	CVE-2020-...	5.0
▼ Apache OpenMeetings (1)							

ページ 1 / 81

割り当てたい侵入防御ルールにチェックを入れて[OK]をクリック

[侵入防御]の一般タブにある[割り当て/割り当て解除]をクリック

6.ポリシー

ポリシー: サーバセキュリティサービス_ポリシー_2 ヘルプ

概要 不正プログラム対策 侵入防御 インタフェースの種類 設定 オーバーライド

一般 詳細 侵入防御イベント

侵入防御

侵入防御のステータス: オン ● 防御, 1つのルール

侵入防御の動作

☒ 防御 ☐ 検出

コンテナの保護

コンテナのネットワークトラフィックの検索: 初期設定 (はい)

現在割り当てられている侵入防御ルール

すべて

割り当て/割り当て解除... プロパティ... エクスポート... アプリケーションの種類... 列...

名前	アプリケーションの種類	優先度	重要度	モード	種類	カテゴリ
1010428 - Apache ActiveMQ U...	ActiveMQ OpenWire	2 - 標準	● 中	防御	攻撃コード	なし

保存 閉じる

選択した「侵入防御ルール」が割り当てられていることを確認して[閉じる]をクリック

6.ポリシー

4. 複製したポリシーを対象のコンピュータに適用する

コンピュータにポリシーを適用した段階で、ポリシーに割り当てたルールがDSAに反映されます

- 対象コンピュータの詳細を表示します。

対象のコンピュータを右クリックし、詳細をクリック

6.ポリシー

- [概要] → [一般] タブの [ポリシー:] のプルダウンから作成したポリシーを選択して保存することで、DSA へ自動でポリシーが配信され、ポリシー適用後に割り当てたルールが DSA へ反映されます。

概要 不正プログラム対策 侵入防御 インターフェース 設定 アップデート オーバーライド	一般	処理	システムイベント	
	ホスト名:	dsa-sss-core		
	表示名:			
	説明:			
	プラットフォーム:	Microsoft Windows Server 2012 R2 (64 bit) Build 9600		
	グループ:	コンピュータ		
	ポリシー:	サーバセキュリティサービス_ポリシー		
	資産の重要度:	> サーバセキュリティサービス_ポリシー サーバセキュリティサービス_ポリシー_2		
セキュリティアップデートのダウンロード:				

6.ポリシー

5. ポリシーで割り当てたルールが適用されていることを確認

- 現在割り当てられている侵入防御ルール数の確認

対象のコンピュータの[詳細] → [侵入防御] → [一般] → [推奨設定]を確認

[現在のステータス:]が、手順1で取得した画面キャプチャまたはメモと比較し、手順3で割り当てたルールの数だけ増えていることを確認

推奨設定	
現在のステータス:	61個の侵入防御ルールが割り当てられています
前回の推奨設定の検索:	2021-08-26 18:34
 未解決の推奨設定:	現在割り当てられている1個のルールの割り当て解除
 備考	割り当て解除が推奨されるルールのうち1個はポリシーレベルで割り当てられているため、割り当て解除にはポリシーエディタを使用する必要があります。

推奨設定の検索によって解除されているルールを適用すると、[未解決の推奨設定:]が表示されます。

[備考]には、手順3でポリシーに割り当てたルール数が表示されます。

6.ポリシー

- 割り当てたルール適用状況の確認

[割り当て/割り当て解除]をクリックし、手順1で取得した画面キャプチャまたはメモと比較して意図したルールにチェックが入っていることを確認。

ポリシーによって割り当てられたルールのチェックボックスはグレイアウトされ、コンピュータからは解除できないようになっています。

現在割り当てられている侵入防御ルール

すべて

割り当て/割り当て解除...

プロパティ...

名前

アプリケーション

侵入防御ルール

すべて

すべて

アプリケーションの種類別

このページを検索

新規

削除...

プロパティ...

複製

エクスポート

アプリケーションの種類...

列...

	名前	優先度	重要度	モード	種類	カテゴリ	CVE	CVSS
▼	ActiveMQ OpenWire (1)							
☑	1010428 - Apache ActiveMQ U...	2 - 標準	● 中	防御	攻撃コード	なし	CVE-2015-...	5.4
▼	Advanced Message Queuing Protocol (AMQP) (1)							
☑	1009126 - Pivotal Spring AMQ...	2 - 標準	● 高	防御	攻撃コード	脆弱性と攻撃コード	CVE-2017-...	7.5
▼	Alibaba Nacos (1)							

6.ポリシー

- 割り当てたルールの設定状況の確認

ルールの変更された場合は、対象のルールをダブルクリックしてプロパティを開き、変更した設定項目を確認し、手順1で取得した画面キャプチャまたはメモと比較して意図した設定になっていることを確認。

The screenshot displays the 'Intrusion Defense Rules' management interface. The main table lists rules for various applications. One rule, '1010428 - Apache ActiveMQ U...', is highlighted with a red box. A red arrow points from this rule to a detailed 'Intrusion Defense Rule Properties' dialog box on the right.

侵入防御ルール

すべて ▼ すべて ▼ アプリケーションの種類別 ▼

新規 ▼ 削除... プロパティ... 複製 エクスポート ▼ アプリケーションの種類 照り列

名前	優先度	重要度	モード	種類	カテゴリ
ActiveMQ OpenWire (1)					
1010428 - Apache ActiveMQ U...	2 - 標準	中	検出のみ	攻撃コード	なし
Advanced Message Queuing Protocol (AMQP) (1)					
1009126 - Pivotal Spring AMQ...	2 - 標準	高	防御	攻撃コード	脆弱性と攻
Alibaba Nacos (1)					
1010971 - Alibaba Nacos AuthF...	2 - 標準	高	防御	攻撃コード	脆弱性と攻
Apache JServ Protocol (2)					
1010184 - Identified Apache JS...	2 - 標準	高	検出のみ	スマート	脆弱性と攻

侵入防御ルールプロパティ 脆弱性 設定 オプション

バージョン: 4.0.0.0

詳細:

アプリケーションの種類: ActiveMQ OpenWire

優先度: 2 - 標準

重要度: 中

モード: 継承(検出のみ)

イベント

☒ 継承

☐ イベントログの無効化

☒ パケット破棄時にイベントを生成

OK キャンセル 適用

7.管理

◆ 概要

- [管理]では、ライセンスの確認やログインユーザの管理、ソフトウェアのアップデートを行えます。

The screenshot displays the Trend Micro Deep Security management console. The left sidebar contains navigation links: システム設定, 予約タスク, イベントベースタスク, ライセンス (selected), ユーザ管理, and アップデート. The main content area is titled 'ライセンス' (License). A green banner indicates the last license update was on 2021-09-06, with a button to 'ステータスをオンラインで確認' (Check status online). Below this is a table with columns: ステータス (Status), 種類 (Type), and 有効期限 (Valid Period). The table lists five items, all with 'アクティベーション完了' (Activation complete) status and an expiration date of 2022-03-31, except for 'Deep Security Scanner' which has 'ライセンスなし' (No license). Each row has a '詳細の表示...' (Show details...) button. At the bottom, there is a button for '新しいアクティベーションコードの入力...' (Enter new activation code...). The bottom right corner shows an 'アラート' (Alert) section with two red indicators.

	ステータス	種類	有効期限	
不正プログラム対策とWebレピュテーション	● アクティベーション完了	製品版	2022-03-31	詳細の表示...
ファイアウォールと侵入防御	● アクティベーション完了	製品版	2022-03-31	詳細の表示...
変更監視とアプリケーションコントロール	● アクティベーション完了	製品版	2022-03-31	詳細の表示...
セキュリティログ監視	● アクティベーション完了	製品版	2022-03-31	詳細の表示...
Deep Security Scanner	● ライセンスなし	なし	なし	詳細の表示...

7.管理

◆ ユーザの管理

- ユーザの追加・削除やパスワードの設定を行えます。

The screenshot displays the Trend Micro Deep Security management console. The top navigation bar includes the Trend Micro logo, the product name 'Deep Security', and links for help, support, and a search bar. Below this, a secondary navigation bar lists various management areas: Dashboard, Processing, Alerts, Events and Reports, Computers, Policies, and Management. The left sidebar contains a tree view of system settings, including System Settings, Scheduled Tasks, Event-based Tasks, Licenses, and User Management. The 'User Management' section is currently selected, showing a list of users. The main content area features a 'Users' header with a role filter dropdown and a search bar. Below this are buttons for adding new users, deleting users, viewing user properties, setting passwords, and listing users. A table lists the users, with columns for Username, Name, Lockout, Login, Last Login, Multi-factor authentication, and Password. One user, 'DS_User (1)', is listed with a green checkmark indicating successful login on 2021-09-06 at 17:05. The bottom right corner shows an alert count of 0.

TREND MICRO | Deep Security

ヘルプ | サポート情報 | ヘルプセンターの検索

ダッシュボード 処理 アラート イベントとレポート コンピュータ ポリシー 管理

システム設定
予約タスク
イベントベースタスク
ライセンス
▼ ユーザ管理
 ユーザ
> アップデート

ユーザ 役割別

このページを検索

新規... 削除... プロパティ... パスワードの設定... 列...

ユーザ名	名前	ロックア...	ログオン	最終ログオン	多要素認...	パスワー...
▼ DS_User (1)						
			✓	2021-09-06 17:05		

アラート 0 0

7.管理

◆ ユーザの新規作成

TREND MICRO | Deep Security

ダッシュボード 処理 アラート イベントとレポート コンピュータ ポリシー **管理**

システム設定
予約タスク
イベントベースタスク
ライセンス
ユーザ管理
ユーザ
アップデート

ユーザ 役割別

新規... 削除...

ユーザ名 ユーザ名

DS_User (1)

一般 連絡先情報 設定

一般情報

ユーザ名 新規ユーザ名

パスワード:

パスワードの確認入力:

備考 このシステムのパスワードの条件は次のとおりです:
・8文字以上であること

名前:

説明:

役割: 役割の選択

言語: 役割の選択

タイムゾーン: Auditor DS_User

時刻の形式: ☐ 12時間 ☒ 24時間

ログオン資格情報

☐ パスワードの有効期限なし

☐ パスワードの複雑性 (パスワードの複雑性)

保存 閉じる

役割の選択
Auditor:
各情報の閲覧のみ可能
DS_User:
各種設定の編集可能

【注意】役割「DS_User」のユーザは削除しないようお願いします

7.管理

◆ アップデート

- セキュリティパッチや、ソフトウェアのアップデートの実施・確認を行えます。

The screenshot shows the 'Deep Security' management interface. The left sidebar contains navigation options: システム設定, 予約タスク, イベントベースタスク, ライセンス, ユーザ管理, アップデート, セキュリティ (selected), ルール, パターンファイル, ソフトウェア, and Relayの管理. The main content area is titled 'セキュリティアップデートの概要' (Security Update Summary). It is divided into two columns: 'パターンファイルアップデート' (Pattern File Updates) and 'ルールアップデート' (Rule Updates). The rows represent different components: 'トレンドマイクロのアップデートサーバ' (Trend Micro Update Server), 'Deep Security', and 'コンピュータ' (Computers). Each row shows the status of updates and provides buttons for further actions.

	パターンファイルアップデート	ルールアップデート
トレンドマイクロのアップデートサーバ	共有されているプライマリテナントのRelayグループが、トレンドマイクロのアップデートサーバからセキュリティアップデートをダウンロードするように設定されています	
Deep Security	✓ 前回のアップデート確認: 2021-09-06 16:06 ✓ 前回のダウンロード: 2021-09-06 16:06	✓ 前回のアップデート確認: 2021-09-06 16:06 ✓ 前回のダウンロード: 2021-09-01 16:18 (21-039) ルールをポリシーに適用... ✓ ポリシーは前回ダウンロードされたルールアップデートを使用しています (21-039)
コンピュータ	⚠ 1台のコンピュータが最新ではありません パターンファイルをコンピュータに送信	✓ コンピュータはすべて最新です ポリシーをコンピュータに送信

8. Appendix

- ◆ コマンドラインの利用
- コマンドラインのうち、サーバセキュリティサービスに有用なコマンドを紹介いたします。

Windowsの場合:

- 管理者権限でコマンドプロンプトを開きます。
- `cd C:\Program Files\Trend Micro\Deep Security Agent\`
- `dsa_control` オプション

Linuxの場合:

- `/opt/ds_agent/dsa_control` オプション

1. ハートビートの送信

`dsa_control -m` : Managerにハートビートを送り、通信を確立します。

※セキュリティアップデート等、管理コンソール上で行った操作はAgentからハートビートが送信された時に実行されます。(初期設定10分毎)管理コンソール上で行った操作をすぐに実行したい場合は、Agentを導入したサーバで上記のコマンドを実行して下さい。

2. Agentの無効化

`dsa_control -r` : Agentを無効化します。

その他のコマンドや詳細につきましては、

<https://help.deepsecurity.trendmicro.com/20.0/on-premise/ja-jp/command-line-interface.html>
をご参照下さい。

8. Appendix

◆ 利用するカーネルに対応したKSPがインポートされているかを確認する方法

1. トレンドマイクロ社が公開しているKSPのReadmeを確認し、ご利用しているカーネルに対応したKSPが公開されているか確認ください。

Deep Security のビルド一覧および日本語版Readme

<https://success.trendmicro.com/ja-jp/solution/ka-0003376>



利用されるDSのバージョンが20.0の場合は「20.0」のリンクをクリック

8. Appendix

2. 利用するカーネルバージョンで検索してください。

例として「Red Hat Enterprise Linux 7: 3.10.0-1160.71.1.el7.x86_64」の場合
カーネルバージョン「3.10.0-1160.71.1.el7.x86_64」で検索します。

以下の図では、赤枠で囲った箇所が対応するKSPのバージョンになります。

20.0.0-4984 Jun. 28, 2022

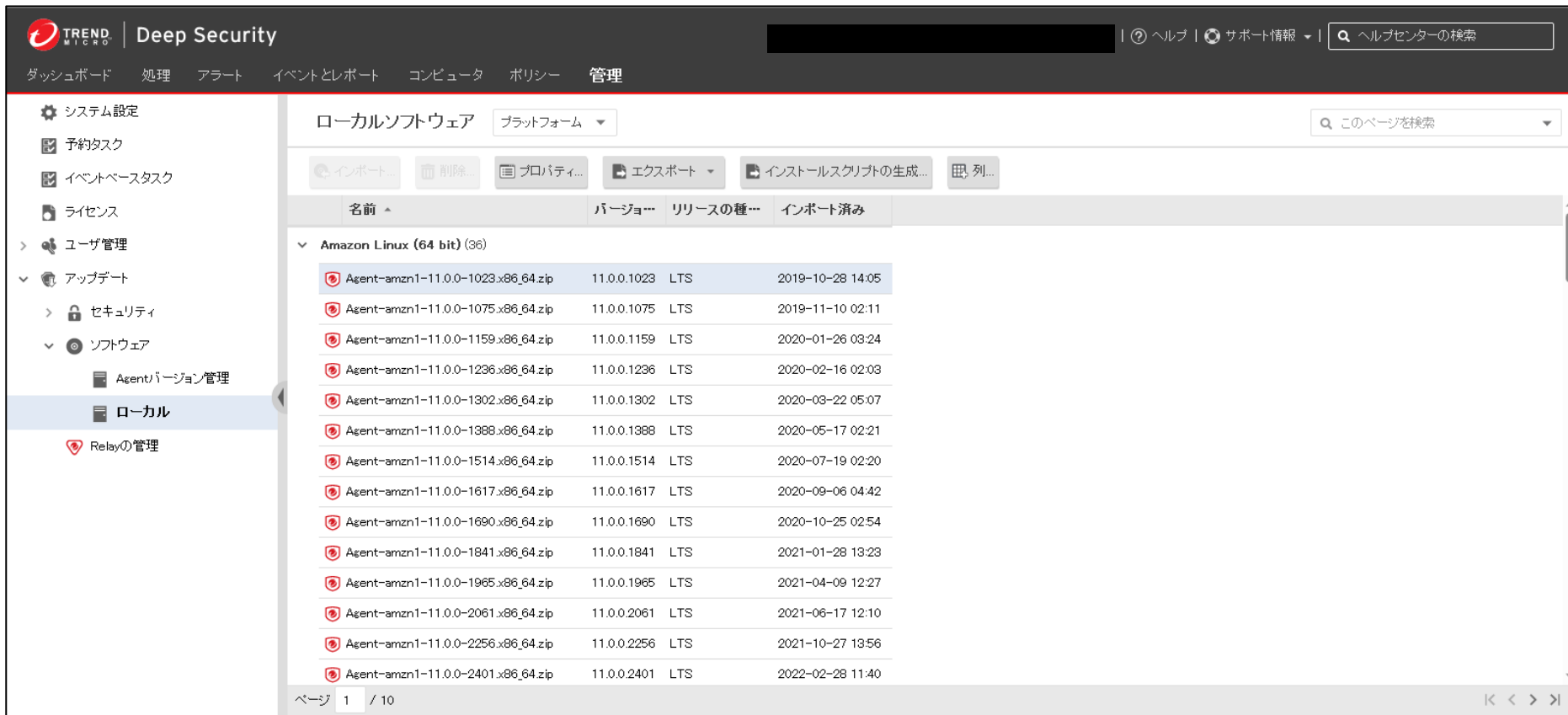
- KernelSupport-RedHat_EL7-20.0.0-4984.x86_64.zip to support
Red Hat Enterprise Linux 7: 3.10.0-1160.71.1.el7.x86_64.

20.0.0-4983 Jun. 28, 2022

- KernelSupport-RedHat_EL8-20.0.0-4983.x86_64.zip to support
Red Hat Enterprise Linux 8: 4.18.0-193.87.1.el8_2.x86_64.

8. Appendix

3. サーバセキュリティサービスのDSM管理コンソールにログインし、以下の画面を表示します。
[管理] - [アップデート] - [ソフトウェア] - [ローカル]



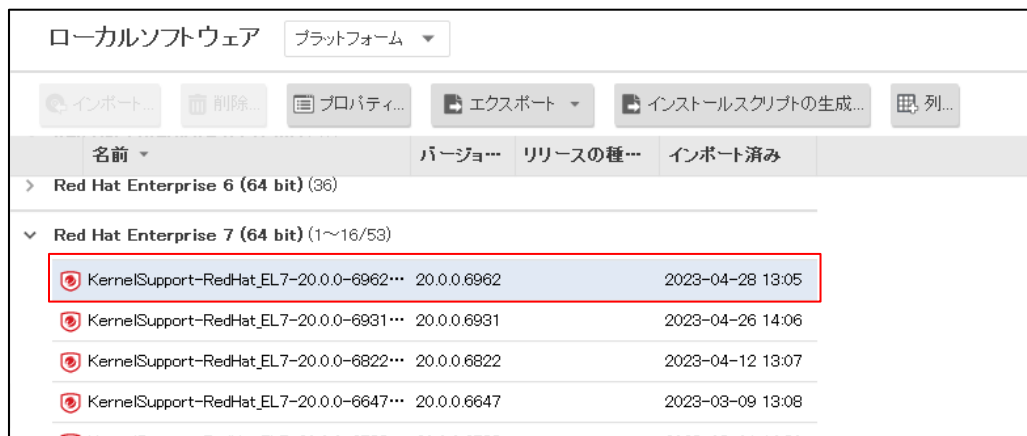
The screenshot shows the Trend Micro Deep Security console interface. The left sidebar contains navigation options: システム設定, 予約タスク, イベントベースタスク, ライセンス, ユーザ管理, アップデート, セキュリティ, ソフトウェア, Agentバージョン管理, ローカル, and Relayの管理. The main area is titled 'ローカルソフトウェア' (Local Software) and shows a list of installed agents for Amazon Linux (64 bit). The table below lists the agents with their names, versions, release types, and import times.

名前	バージョン	リリースの種類	インポート済み
Amazon Linux (64 bit) (36)			
Agent-amzn1-11.0.0-1023.x86_64.zip	11.0.0.1023	LTS	2019-10-28 14:05
Agent-amzn1-11.0.0-1075.x86_64.zip	11.0.0.1075	LTS	2019-11-10 02:11
Agent-amzn1-11.0.0-1159.x86_64.zip	11.0.0.1159	LTS	2020-01-26 03:24
Agent-amzn1-11.0.0-1236.x86_64.zip	11.0.0.1236	LTS	2020-02-16 02:03
Agent-amzn1-11.0.0-1302.x86_64.zip	11.0.0.1302	LTS	2020-03-22 05:07
Agent-amzn1-11.0.0-1388.x86_64.zip	11.0.0.1388	LTS	2020-05-17 02:21
Agent-amzn1-11.0.0-1514.x86_64.zip	11.0.0.1514	LTS	2020-07-19 02:20
Agent-amzn1-11.0.0-1617.x86_64.zip	11.0.0.1617	LTS	2020-09-06 04:42
Agent-amzn1-11.0.0-1690.x86_64.zip	11.0.0.1690	LTS	2020-10-25 02:54
Agent-amzn1-11.0.0-1841.x86_64.zip	11.0.0.1841	LTS	2021-01-28 13:23
Agent-amzn1-11.0.0-1965.x86_64.zip	11.0.0.1965	LTS	2021-04-09 12:27
Agent-amzn1-11.0.0-2061.x86_64.zip	11.0.0.2061	LTS	2021-06-17 12:10
Agent-amzn1-11.0.0-2256.x86_64.zip	11.0.0.2256	LTS	2021-10-27 13:56
Agent-amzn1-11.0.0-2401.x86_64.zip	11.0.0.2401	LTS	2022-02-28 11:40

8. Appendix

4. 一覧からご利用のOSをクリックして、インポートされている最新KSPをご確認ください。

OSが「Red Hat Enterprise Linux 7」でDSAのバージョンが20.0の場合
「KernelSupport-RedHat_EL7-20.0.0-<ビルド番号>.x86_64.zip」の
<ビルド番号>が一番大きいものを確認します。



手順2で確認したバージョンと一致しているため、利用するカーネルに対応したKSPがインポートされていると判断できます。

新しいKSPには古いKSPのサポートも含まれるため手順2で確認したバージョンより大きい場合も、利用するカーネルに対応したKSPがインポートされていると判断できます。

9.注意事項

- 不正プログラム対策機能をご利用のお客様

不正プログラム対策機能により不審なファイルが隔離された場合、通信方向が[Agent/Applianceから開始]となっている為、管理コンソール上では削除できません。
本項では隔離ファイルの処理方法を紹介します。

- ファイルが隔離処理された場合の対応方法

1. サーバのローカルで隔離ファイルを削除
2. Managerから隔離イベントを削除

※ 隔離されたファイルは暗号化されてファイル名が変更されるため、サーバ上で隔離ファイルの生成日時と管理コンソール上の検出ファイルの時刻を比較してそれぞれ削除が必要となります。

・隔離ファイルや隔離の動作に関するよくあるお問い合わせ

<https://success.trendmicro.com/ja-jp/solution/ka-0005972>

・通信方向が[Agent/Applianceから開始]の場合の制限事項について

<https://success.trendmicro.com/ja-jp/solution/ka-0005792>

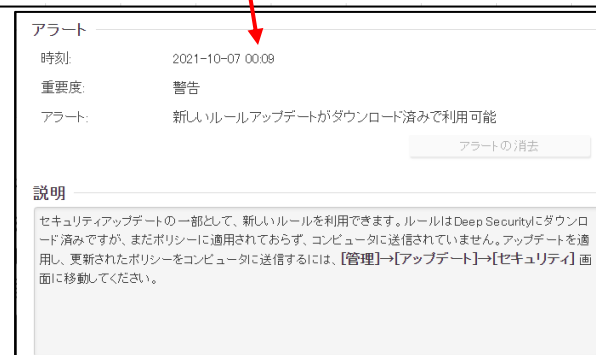
9. 注意事項

- 「新しいルールアップデートがダウンロード済みで利用可能」アラート発生時の対応について

Managerのリソースに対して一時的な負荷が発生し、新しいルールのポリシー反映までに時間を要したためアラートが発令されたと考えられます。

ポリシー反映完了後、アラートは解除されますので対処は不要です。

※アラートメールでは「新しいアラートの発令:新しいルールアップデートが未適用です」の件名でメールが送付されます。



9.注意事項

- Trend Micro Vision One (XDR)について
バージョン20.0から[管理]>[システム設定]に[Trend Micro Vision One]タブが追加されていますが、本サービスでは提供していませんので触らないようにしてください。



10.問い合わせ先

- 購入済みのお客様
NEC PPサポートサービスをご利用ください。

Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

\Orchestrating a brighter world

NEC